Trust Technology Assessment Program

EVALUATION TECHNICAL REPORT

LUCENT TECHNOLOGIES

LUCENT MANAGED FIREWALL (LMF) 4.0

PREPARED BY:

COMPUTER SCIENCES CORPORATION
7471 CANDLEWOOD ROAD
HANOVER, MD 21076

SUBMITTED TO:
TTAP OVERSIGHT BOARD

VERSION 1.1
FEBRUARY 2000

APPROVED FOR PUBLIC RELEASE;

DISTRIBUTION UNLIMITED

FOREWORD

This publication, the Lucent Technologies Lucent Managed Firewall (LMF) 4.0, Evaluation Technical Report is being issued by Computer Sciences Corporation. This report is the principle source of information used by the Trust Technology Assessment Program (TTAP) Oversight Board to render a certification rating for the Lucent Technologies Lucent Managed Firewall (LMF) 4.0 product. It is intended to support the TTAP certification process by providing all the information needed by the TTAP Oversight Board to verify the results of the evaluation. This report presents all evaluation results, their justifications and any findings derived from the work performed during the evaluation. The requirements stated in this report are taken from the *Lucent Managed Firewall (LMF) 4.0 Security Target, Version 1.0* and are conformant with the *Common Criteria for Information Technology Security Evaluation, Version 2.0*.

Hard copy signed

Director, TTAP Evaluation Facility

Hard copy signed

Quality Manager, TTAP Evaluation Facility

Table of Contents

LIST OF TABLES

LIST OF FIGURES

LUCENT TECHNOLOGIES LUCENT MANAGED FIREWALL VERSION 4.0 EVALUATION TECHNICAL REPORT

1 INTRODUCTION

1.1 Identification

1 Table 1 provides information needed to identify and control this Evaluation Technical Report (ETR), the Security Target (ST) and the Target of Evaluation (TOE). This table also identifies the key players involved with the evaluation.

Table 1: Evaluation Identifiers

Item	Identifier
Evaluation Scheme	United States Trust Technology Assessment Program
Evaluation Technical Report	Lucent Technologies Lucent Managed Firewall Version 4.0 Evaluation Technical Report, January 2000, Version 1.0
Security Target	Lucent Managed Firewall Version 4.0 Security Target, Version 1.0
Protection Profile	U.S. Government Traffic-Filter Firewall Protection Profile for Low-Risk Environments, Version 1.1, April 1999
Target of Evaluation	Lucent Managed Firewall Version 4.0 Build 199 executing on Microsoft Windows NT 4.0 Service Pack 4 and Brick Model 201
EAL	2
Developer	Lucent Technologies
Sponsor	Lucent Technologies
Evaluators	Computer Sciences Corporation Lindon Bailey Kimberly Caplan H. Patrick Dunn, CISSP Vince Ritts Douglas Stuart, CISSP Government Participants Steve Monaco
Certifers	Mario Tinto Rita Montequin

1.2 Background

2 The TTAP is a joint National Security Agency (NSA) and National Institute of Standards and Technology (NIST) effort to establish commercial facilities to perform trusted

product evaluations. Under this program, security evaluations are conducted by commercial testing laboratories called TTAP Evaluation Facilities (TEFs) using the current NSA evaluation methodology and proposed evaluation methodology for Evaluation Assurance Level (EAL) 1 and EAL 2 in accordance with cooperative research and development agreements. The program focuses on products with features and assurances characterized by the Common Criteria (CC) EAL 1 through EAL 4. In addition, TEFs are allowed to conduct PP evaluations.

3 The TTAP Oversight Board assigns a Certifier(s) to monitor the TEFs to ensure quality and consistency across evaluations. Developers of information technology products desiring a security evaluation contract with a TEF and pay a fee for their product's evaluation. Upon successful completion of the evaluation, the product is be added to NSA's Evaluated Products List.

4 The TTAP is migrating to the National Information Assurance Partnership (NIAP) Common Criteria Evaluation and Validation Scheme (CCEVS). Under the Mutual Recognition Arrangement (MRA), evaluation facilities conducting CC evaluations must apply the Common Evaluation Methodology (CEM). In anticipation of the final version of the CEM and its application, the TTAP Oversight Board has requested all TEFs to use the CEM when conducting CC evaluations, as appropriate.

1.3 References

5 The following documents are referenced throughout this report.

[CC_PART1]	Common Criteria for Information Technology Security Evaluation – Part 1: Introduction and general model, dated May 1998, version 2.0.
[CC_PART2]	Common Criteria for Information Technology Security Evaluation – Part 2: Security functional requirements, dated May 1998, version 2.0.
[CC_PART2A]	Common Criteria for Information Technology Security Evaluation – Part 2: Annexes, dated May 1998, version 2.0.
[CC_PART3]	Common Criteria for Information Technology Security Evaluation – Part 3: Security assurance requirements, dated May 1998, version 2.0.
[CEM_PART1]	Common Evaluation Methodology for Information Technology Security – Part 1: Introduction and general model, dated 1 November 1998, version 0.6.
[CEM_PART2]	Common Evaluation Methodology for Information Technology Security – Part 2: Evaluation Methodology, dated January 1999, version 0.6
[LMF2_IND]	Lucent Managed Firewall Version 4.0 Independent Testing Report

[LMF2_PEN]	Lucent Managed Firewall Version 4.0 Penetration Testing Report
[LMF2_ST]	Lucent Managed Firewall (LMF), Version 4.0, Security Target, Version 1.0
[TFF_PP]	U.S. Government Traffic-Filter Firewall Protection Profile for Low-Risk Environments, April 1999, Version 1.1

1.4 Document Organization

6 This ETR is organized according to the structure dictated by the Common Evaluation Methodology (CEM) Version 0.6 on page 14, Figure 2.2. All the sections of this ETR conform to the ETR requirements described in the CEM and is divided into the following Chapters:

7 Chapter 1 Introduction, describes the background of the Scheme, identifies the ETR, ST and TOE control identifiers, and identifies the developer, sponsor, evaluators, and certifiers of the evaluation;

8 Chapter 2 Architectural Description, provides a high-level description of the TOE and its major components;

9 Chapter 3 Evaluation, describes the methods, techniques, tools, and standards used during the evaluation; constraints or assumptions regarding the conduct and results of the evaluation; and identifies the evaluation evidence examined;

10 Chapter 4 Results of the Evaluation, provides a verdict and supporting rationale for each assurance component completed for the evaluation;

11 Chapter 5, Conclusions and Recommendations;

12 Chapter 6, Acronyms and Glossary; and

13 Chapter 7, Problem Reports, lists the Evaluation Discovery Reports (EDRs) and Observation Reports (ORs) that were raised during the evaluation and their status.

2 ARCHITECTURAL DESCRIPTION OF THE TOE

14 This section describes the high-level design of the LMF and NT subsystems and identifies their interfaces. The information presented is not intended to describe the complete design of each subsystem, but rather to provide sufficient information to enable the reader to understand the LMF design and provide evidence that the system satisfies its functional requirements.

15 The LMF is a security system consisting of one or more Firewall Appliance(s) to mediate information transfer between domains and a Security Management Server (SMS) to administer the firewall appliance.

16 The firewall function is physically separated from its management server, with the firewall code running on Inferno™, a small Bell Labs-developed operating system. The SMS software runs on a separate Windows NT™ platform.

17 The Firewall Appliance (FA) executes LMF FA, Version 4.0 software on Model 201 hardware. This software consists of the Inferno™ operating system and simple firewall code that is embedded within the operating system kernel.

18 The FA Model 201 hardware is based on the Intel Pentium platform. The FA is equipped with four auto-sensing 10/100Base-T Ethernet interface cards and can be positioned between any type of Ethernet-based network elements (e.g., routers, hubs, switches, servers, PCs). Because the FA is a bridge-level device, these network interfaces do not have IP addresses, thus rendering the FA invisible to the other network elements.

19 The FA does not contain a hard drive and can be deployed without a monitor and keyboard. Other than a floppy disk drive for initial software boot, it has a minimum of moving parts (an on/off switch and a power supply fan).

20 The Inferno operating system (OS) itself has no user accounts or file system. The Inferno OS in this evaluation is a dedicated specially designed version that just has firewalling capability. This means it does not support user accounts nor does it have any general purpose computing capability. The firewall operating system and firewall application fit onto a single 3.5-inch floppy diskette.

21 The fact that the Inferno OS is a special purpose OS as described above helps satisfy the non-bypassibility functionality of the TOE. The non-bypassability of the TOE is enforced at the networking interfaces to the TOE. That is the RFCs that control the flow of information at the networking interface do not allow for the bypassing of the TSF. The way the RFCs are implemented does not allow the flow of network traffic to bypass what the protocol specifies is supposed to happen. Further, the requirement for separation of domains is satisfied because there are no processes running on the hardware that are non-firewall processes.

22 The FA software:

- performs security policy enforcement on packets crossing its interfaces based on one or more Security Policies, and

- collects audit session statistics, establishes virtual private networks between Firewall Appliances.

23 Figure 1 below shows a typical environment. The domain, “Other Protected Network” is included to show that the TOE has the capability to distinguish between three network domains. However, the evaluated configuration consisted only of the domains, “Protected Network” and “External Network”.

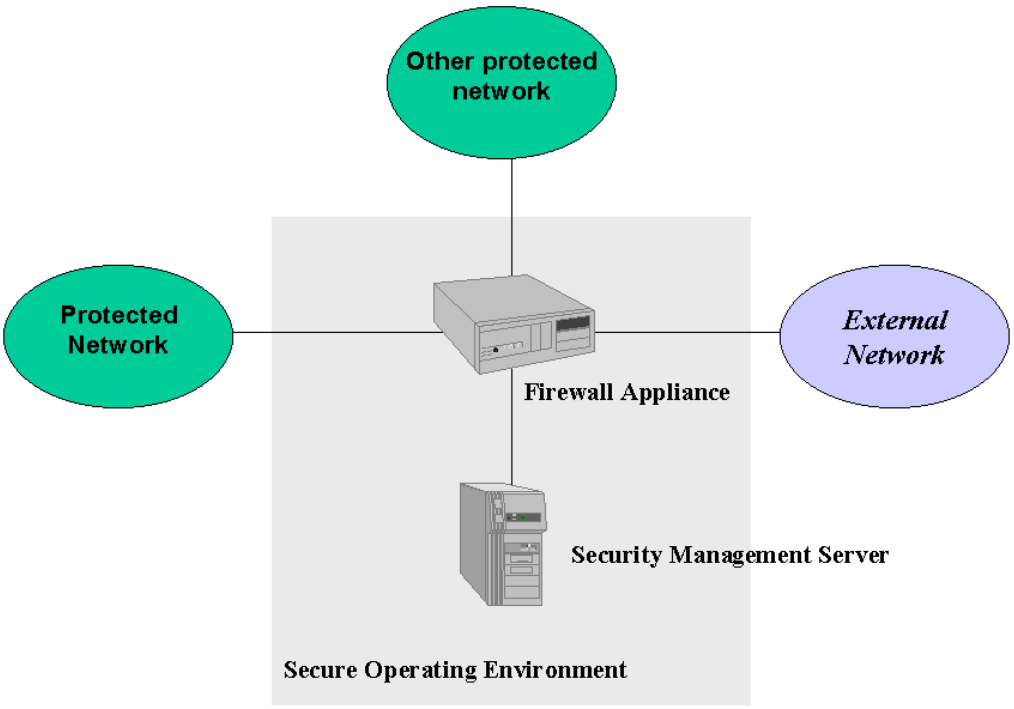

Figure 1: Secure Operating Environment

2.1 LMF Subsystems

24 The following sections describe the subsystems of the LMF.

25 The LMF is comprised of nine (9) subsystems. Figure 2 identifies the subsystems. It is indicated in Figure 2 that certain subsystems can communicate across a network. However, such connections are not allowed in the evaluated configuration; the evaluated configuration does not support either remote administration or the encryption of links between elements of the TOE. The SMS is composed of the box labeled ‘Client GUI’ and all the subsystems in the box below labeled ‘Part of SMS’. In the evaluated configuration, the management server resides on a separate hardware platform, and is connected to the Firewall Appliance via a private network connection. The BRICK is the Firewall Appliance. VPN is virtual private network, which is not part of this evaluation.

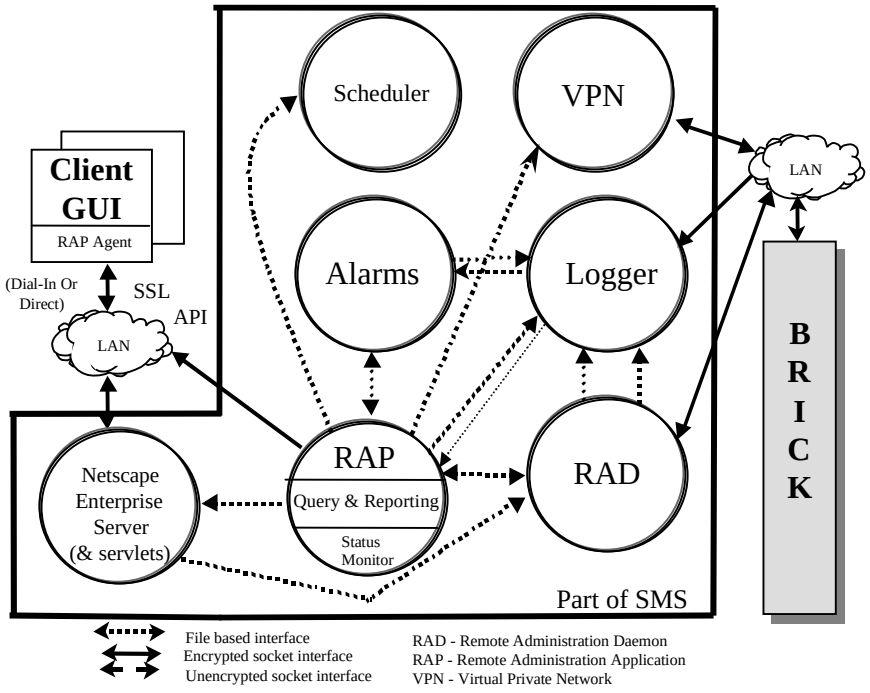

Figure 2: Subsystem Diagram

2.1.1 GUI Client/Graphical User Interface Subsystem

26 The NT Workstation Client/Graphic User Interface (GUI) Subsystem manages the authorized administrator's SMS login, supports software (applet) download, displays data, and manages user data flow. These capabilities enable an Administrator or Zone Administrator to access the SMS on the system console.

27 The Client/GUI Subsystem displays data to the administrator using a Netscape Communicator 4.05 web browser with Java™ enabled.

2.1.2 Netscape Enterprise Server Subsystem

28 The Netscape Enterprise Server (NES) Subsystem is a COTS web server, Netscape Enterprise Server, Version 3.5.1. The NES Subsystem authenticates itself to Client/GUI Subsystem using a VeriSign digital certificate, provides SSL services to protect user authentication and session data, provides Java™ services to facilitate Login Servlet execution and software downloading, enforces access control on help and product documentation web pages, and hosts report documents. The NES Subsystem supports Java™ Version 1.1.5 (W/JPP).

2.1.3 Remote Administration Application Subsystem

29 The Remote Administration Application (RAP) Subsystem manages the interface between itself and the Client/GUI Subsystem. It performs session management, performs edits to data, requests reports, routes console messages to the Client/GUI Subsystem, generates and routes monitor messages to the Client/GUI Subsystem, and logs the

administrator out when unhandled errors occur. The RAP Subsystem manages the administrator session while communicating with the SMS. This includes supporting the establishment of a secure session between itself and the Client/GUI Subsystem and simultaneously managing multiple user threads.

30 The RAP Subsystem manages the administrator interface. This includes interacting with the user management screens presented within the Client/GUI JVE to provide the appropriate Java™ Applet in response to administrator input. Such interactions include management of user accounts, alarms, logging, and zone management.

31 The addition, deletion, and modification of SMS user accounts (i.e., administrator) are audited by the SMS. The audit record generated will identify the administrator performing the action, when it took place, and the administrator account that was added, deleted, or modified.

32 The TOE consists of two primary pieces that run different OSs; the SMS and the Brick. The SMS is a Windows NT™ workstation while the Brick is a platform that is running the Inferno OS. User accounts (i.e., administrator) only exist on the SMS. Since the SMS runs Windows NT™ it has the capability of maintaining users accounts; for this evaluation the only user accounts on the SMS are those who administer the TOE, i.e. trusted users. The Inferno OS on the other hand, does not have user accounts on it.

33 Creating Zone Security Policies is a restricted function that can only be performed by System and Zone Administrators. System Administrators can create, modify or delete any Zone Security Policy. Zone Administrators can create, modify or delete only the Zone Security Policy for the security zone they manage.

2.1.4 Remote Administration Daemon Subsystem

34 The Remote Administration Daemon (RAD) Subsystem performs Administrator Account Management, Firewall Interface and Management, Zone Management, and Policy Compilation. The RAD Subsystem has been developed using hosted Inferno™, has built-in authentication (key-exchange engine), is a threaded architecture, and talks to other subsystems via a file or socket interface.

2.1.5 Alarms Subsystem

35 The Alarms Subsystem provides the LMF System with a real-time alarming capability.

2.1.6 Logger Subsystem

36 The Logger Subsystem creates a non-volatile record of events affecting security, management, or maintenance of the LMF.

37 SMS backup is performed using NT operating system commands. The ability to perform backup in NT is restricted to users in the Administrator group. The only users that can access the TOE are users with these permissions. The backup of the SMS preserves all FA configuration information.

38 SMS backup recovery is performed using NT operating system commands. The ability to perform backup and recovery in NT is restricted to users in the Administrator group. The only users that can access the TOE are users with these permissions. The restoration of FA services can be accomplished using that FA's information that is preserved and backed-up on the SMS.

2.1.7 Firewall Appliance Subsystem

39 The Firewall Appliance (FA) Subsystem is equipped with four auto-sensing 10/100Base-T Ethernet interface cards and can be positioned between any type of Ethernet-based network elements (e.g., routers, hubs, switches, servers, PCs).

2.1.8 Virtual Private Network Gateway Controller Subsystem

40 The Virtual Private Network (VPN) Gateway Controller Subsystem provides authentication of a VPN client and sets up a tunnel for the client once it is authenticated.

2.1.9 Scheduler Subsystem

41 The Scheduler Subsystem runs programs at specified intervals.

3 EVALUATION

3.1 Evaluation Methods, Techniques, and Standards

42 The *evaluator action elements* documented in [CC_PART3] for EAL 2 assurance components was the basis of the approach for evaluating the TOE. In addition, [CEM_PART2] Chapter 6 was used to define the specific evaluator actions for conducting the evaluation.

43 To manage the evaluation effort and to document progress and findings, the evaluation team developed evaluation work package reports for each assurance family as listed in Table 2. All CEM work units associated with these assurance components were completed and addressed as instructed by the Scheme.

Table 2: Evaluation Work Packages

Work Package	Assurance Component
Security Target	ASE
Configuration Management	ACM_CAP.2
Delivery and Operation	ADO_DEL.1
	ADO_IGS.1
Development	ADV_FSP.1
	ADV_HLD.1
	ADV_RCR.1
Guidance Documents	AGD_ADM.1
	AGD_USR.1
Tests	ATE_COV.1
	ATE_FUN.1
	ATE_IND.2
Vulnerability Assessments	AVA_SOF.1
	AVA_VLA.1
Assurance Maintenance	AMA_AMP.1
	AMA_CAT.1

44 For the ATE_IND.2.2E evaluator action element, the evaluation team wrote a test plan and conducted functional testing in accordance with the plan. For the AVA_VLA.1.2E evaluator action element, the evaluation team coordinated with the PP author to identify the current list of obvious vulnerabilities. The team wrote a test plan for penetration testing and conducted tests in accordance with the plan.

45 Throughout the evaluation, the evaluation team generated Observation Reports (ORs) to request clarification on the [TFF_PP] or Common Criteria requirements. ORs were submitted to the Certifier for posting and resolution. Evaluation Discovery Reports (EDRs) were generated for the following reasons:

- To identify a potential vulnerability or deficiency found in the TOE;
- To identify deficiencies found in evaluation evidence; and
- To request additional information from the vendor.

46 EDRs were submitted to the vendor and not formally distributed to the TTAP Oversight Board, although the Certifier did receive a copy of all EDRs. Chapter 7, Problem Reports, contains a listing of all ORs and EDRs that were generated during the evaluation.

3.2 Evaluation Tools

47 To perform independent and penetration testing activities, the evaluation team used network tools:

- to observe the success or failure of information flows through the TOE based on flow rules;
- to examine packet information at all protocol layers for residual information; and
- to manipulate network and application layer flows to simulate various attack scenarios.

3.3 Evaluation assumptions and constraints

48 The evaluation results and evidence will be maintained and retired as specified in CSC's Common Criteria Evaluation Laboratory Quality Manual.

3.4 Evaluation Deliverables

49 Table 3 provides a listing of evidence supplied as evaluation deliverables.

Table 3: Evaluation Deliverables

Identifier	Date of Receipt	Issuing Body	Title
[BRICK]	19 Aug 1999	Lucent Technologies	Lucent Managed Firewall Model 201
[LMF2_ACM]	30 Aug 1999	Lucent Technologies	Lucent Managed Firewall, Version 4.0, Configuration Management, Version 2.0
[LMF2_ADM]	30 Aug 1999	Lucent Technologies	Lucent Managed Firewall, Version 4.0, Administrator Guidance, Version 1.0
[LMF2_AMP]	Nov 1999	Lucent Technologies	Lucent Managed Firewall, Version 4.0, Assurance Maintenance (AM) Plan, Version 1.0
[LMF2_AVA]	21 Oct 1999	Lucent Technologies	Lucent Managed Firewall, Version 4.0, Vulnerability Analysis, Version 2.1
[LMF2_CAT]	Nov 1999	Lucent Technologies	Lucent Managed Firewall, Version 4.0, Categorization Report, Version 1.0
[LMF2_COV]	15 Nov 1999	Lucent Technologies	Lucent Managed Firewall Version 4.0 Functional Testing, Version 2.2
[LMF2_FAIL]	4 Oct 1999	Lucent Technologies	Lucent Managed Firewall R4.0 SMS Failover Test Plan
[LMF2_FSP]	19 Nov 1999	Lucent Technologies	Lucent Managed Firewall, Version 4.0, Functional Specification, Version 2.2
[LMF2_HLD]	19 Nov 1999	Lucent	Lucent Managed Firewall, Version 4.0, High-

		Technologies	Level Design Document, Version 2.2
[LMF2_IGS]	26 Oct 1999	Lucent Technologies	Lucent Managed Firewall, Version 4.0, Delivery, Installation, Generation, and Start-Up Procedures, Version 8.3
[LMF2_MAN1]	19 Aug 1999	Lucent Technologies	Lucent Technologies, Bell Labs Innovations, Lucent Security Management Server v4.0(i), System Administrator Reference Manual
[LMF2_MAN2]	19 Aug 1999	Lucent Technologies	Lucent Technologies, Bell Labs Innovations, Lucent Security Management Server v4.0(i), Zone Administrator Reference Manual
[LMF2_MAN3]	19 Aug 1999	Lucent Technologies	Lucent Technologies, Bell Labs Innovations, v4.0(i), Lucent Proxy Agent Installation and User Guide
[LMF2_MAN4]	19 Aug 1999	Lucent Technologies	Lucent Technologies, Bell Labs Innovations, Lucent Security Management Server v4.0(i), Model 201 Brick Specifications
[LMF2_MAN5]	19 Aug 1999	Lucent Technologies	Lucent Technologies, Bell Labs Innovations, Lucent Security Management Server v4.0(i), Setup and Configuration Guide
[LMF2_MAN6]	19 Aug 1999	Lucent Technologies	Lucent Technologies, Bell Labs Innovations, Lucent Security Management Server v4.0(i), Installation Guide
[LMF2_PRO]	2 Aug 1999	Lucent Technologies	Lucent Managed Firewall R4.0 Proactive Monitoring Feature Test Plan
[LMF2_RCR]	19 Nov 1999	Lucent Technologies	Lucent Managed Firewall, Version 4.0, Correspondence Document, Version 2.1
[LMF2_REG]	20 Oct 1999	Lucent Technologies	Lucent Managed Firewall v4.0 Regression Test Plan
[LMF2_SOFT]	3 Dec 1999	Lucent Technologies	LSMS Build 199
[LMF2_ST]	29 July 1999	Lucent Technologies	Lucent Managed Firewall (LMF), Version 4.0, Security Target, Version 1.0
[LMF2_UMA]	29 July 1999	Lucent Technologies	LMF V4.0 User Model and Authentication Testing
[LMF2_URL]	29 July 1999	Lucent Technologies	Lucent Managed Firewall Release 4.0 Content Security - URL Blocking/Filtering Testing
[LMF2_VIR]	29 July 1999	Lucent Technologies	Internet Security Products Group, Lucent Managed Firewall, Release 4.0, Lucent Proxy Agent- Virus Scanning Test Plan
[NIC]	22 Nov 1999	Lucent Technologies	Network interface cards
[TFF_PP]	N/A	NSA	U.S. Government Traffic-Filter Firewall Protection Profile for Low-Risk Environments, April 1999, Version 1.1

4 RESULTS OF THE EVALUATION

50 This Chapter presents the findings and results of the evaluation by identifying the verdict with supporting rationale for each assurance component that constitutes an activity for the ST Evaluation and EAL 2 Evaluation. A verdict for an assurance component is determined by the resulting verdicts assigned to the corresponding evaluator action elements. Three mutually exclusive verdict states can be rendered:

- *Pass*, if the evaluator successfully completes a [CC_PART3] evaluator action element. The conditions for successfully completing an evaluator action element are defined by the constituent work units of the related [CEM_PART2] action.

- *Inconclusive*, if the evaluator has not completed one or more work units of the [CEM_PART2] action related to the [CC_PART3] evaluator action element.

- *Fail*, if the evaluator unsuccessfully completes a [CC_PART3] evaluator action element.

51 Section 5 provides the overall verdict of the evaluation team's findings as defined in [CC_PART1] Chapter 5, and determined by the verdict assignments presented in this Chapter.

52 Table 4 provides a listing of the activities, associated assurance components, and evaluator action elements for a ST Evaluation and an EAL 2 Evaluation. A detailed description of the actions taken by the evaluation team to complete each evaluator action element for each assurance component can be found in the set of work package reports, which were provided to the Certifier under a separate cover.

Table 4: Evaluation Activities, Assurance Components, and Action Elements

Activity	Assurance Component	Evaluator Action Elements
ST Evaluation	ASE_DES.1	ASE_DES.1.1E, ASE_DSE1.2E, ASE_DES1.3E
	ASE_ENV.1	ASE_ENV.1.1.E, ASE_ENV.1.2E
	ASE_INT.1	ASE_INT.1.1E, ASE_INT.1.2E, ASE_INT.1.3E
	ASE_OBJ.1	ASE_OBJ.1.1E, ASE_OBJ.1.2E
	ASE_PPC.1	ASE_PPC.1.1E, ASE_PPC.1.2E
	ASE_REQ.1	ASE_REQ.1.1E, ASE_REQ.1.2E
	ASE_SRE.1	ASE_SRE.1.1E, ASE_SRE.1.2E
	ASE_TSS.1	ASE_TSS.1.1E, ASE_TSS.1.2E
Configuration management	ACM_CAP.2	ACM_CAP.2.1E
Delivery and operation	ADO_DEL.1	ADO_DEL.1.1E, Implied Action
	ADO_IGS.1	ADO_IGS.1.1E, ADO_IGS.1.2E
Development	ADV_FSP.1	ADV_FSP.1.1.E, ADV_FSP.1.2E
	ADV_HLD.1	ADV_HLD.1.1E, ADV_HLD.1.2E
	ADV_RCR.1	ADV_RCR.1.1E
Guidance documents	AGD_ADM.1	AGD_ADM.1.1E

Activity	Assurance Component	Evaluator Action Elements
	AGD_USR.1	AGD_USR.1.1E
Tests	ATE_COV.1	ATE_COV.1.1E
	ATE_FUN.1	ATE_FUN.1.1E
	ATE_IND.2	ATE_IND.2.1E, ATE_IND.2.2E, ATE_IND.2.3E
Vulnerability assessment	AVA_SOF.1	AVA_SOF.1.1E, AVA_SOF.1.2E
	AVA_VLA.1	AVA_VLA.1.1E, AVA_VLA.1.2E
Assurance Maintenance	AMA_AMP.1	AMA_AMP.1.1E, AMA_AMP.1.2E
	AMA_CAT.1	AMA_CAT.1.1E, AMA_CAT.1.2E

4.1 Security Target Evaluation Results

53 The objective of the ST evaluation is to determine whether [LMF2_ST] is complete, consistent, technically sound, and to determine that the [LMF2_ST] provides a suitable baseline for evaluation of the TOE. In addition, the ST is also examined to verify its protection profile conformance claim to the [TFF_PP].

4.1.1 ASE_DES.1 – TOE Description

54 The evaluator reviewed the TOE description section of the Lucent Managed Firewall (LMF), Version 4.0, Security Target, Version 1.0 to make a determination that the section describes the Lucent Managed Firewall version 4.0, the TOE. The TOE description defines the boundaries of the TOE in both a physical and logical way. It was clear to the evaluator after reading the TOE description that the product was a traffic filter firewall product.

55 The TOE description was checked for consistency by looking for any contradictory statements that might appear within this section of the ST. No statements were found while examining the TOE description that contradicted each other.

56 The TOE description was checked for consistency with other sections of the ST. This consistency check was performed in conjunction with the other ASE work units. The description given of the functionality and assurance measures of the TOE are consistent throughout the whole ST.

57 ***ASE_DES.1 Verdict:***

58 The evaluation team concluded that the TOE has met the assurance requirements of ASE_DES.1. Therefore, a **pass** verdict has been issued for this assurance component.

4.1.2 ASE_ENV.1 – Security environment

59 The security environment section of the [LMF2_ST] was used to satisfy this assurance component. The evaluator reviewed this section to determine that it identifies the assumptions and threats for the TOE and its environment. The [LMF2_ST] does not contain any organizational security policies.

60 The evaluator developed tables to help satisfy the evaluator action elements of this assurance component. A table for the assumptions was developed and a table for the threats was developed. The tables also were used to determine if the assumptions and threats being articulated in the [LMF2_ST] were the same or varied from the [TFF_PP]. The tables allowed the evaluator to track which assumption or threat they were reviewing and to note any issues that the evaluator might have with an assumption or threat in the [LMF2_ST] while reviewing that assumption or threat.

61 While reviewing the individual assumptions and threats the evaluator was also determining if the assumptions and threats were coherent, understandable to the evaluator and the audience for the [LMF2_ST]. An overall consistency verdict was reached after all the assumptions and threats had been reviewed. Part of the consistency check was to make sure that no assumptions are in conflict with the threats and that the threats, as specified, are plausible based on the threat agents described, the attack and the asset that could be under attack.

62 ***ASE_ENV.1 Verdict:***

63 The evaluation team concluded that the TOE has met the assurance requirements of ASE_ENV.1. Therefore, a **pass** verdict has been issued for this assurance component.

4.1.3 ASE_INT.1 – ST introduction

64 The evaluator reviewed the security target introduction section of the [LMF2_ST] to satisfy the evaluator elements of this assurance component. The ST introduction of the [LMF2_ST] clearly identifies the [LMF2_ST] with a name and version for the [LMF2_ST]. Along with the [LMF2_ST] identification it also gives a unique label with a version number for the TOE under evaluation. The CC version used to develop the ST is clearly identified in the [LMF2_ST].

65 Part of the evaluation of the [LMF2_ST] introduction was to determine if it contained a narrative description of the [LMF2_ST]. The [LMF2_ST] clearly states what is in the [LMF2_ST]. It is stated in such a manner and to a level that is clear that a traffic filter firewall product is being described and the type of functionality that is being provided by the TOE.

66 The [LMF2_ST] introduction clearly states the conformance claims of the [LMF2_ST]. It mentions the [TFF_PP] and the relevant Part 2 and 3 conformance claims to the CC.

67 The evaluator determined that the [LMF2_ST] introduction is coherent by reading the section and being able to understand what was being described in the section. Further it was determined that the section was consistent because the statements of functionality and use of terms in this section did not conflict with each other.

68 It was determined that the [LMF2_ST] introduction is consistent with the other sections of the [LMF2_ST]. The determination of consistency with the other sections of the [LMF2_ST] was undertaken while working on the other evaluator actions in other ASE components. The evaluator checked for consistency in the [LMF2_ST] by reviewing all the other sections of the [LMF2_ST]. The evaluator looked for any conflict between the description of functionality through out the different sections of the [LMF2_ST]. This included looking at the functional requirements and the security functions described in

the TOE summary specification. The words of the assumptions, threats, and objectives were compared with each other and the functional requirements to determine that they did not conflict with each other.

69 ***ASE_INT.1 Verdict:***

70 The evaluation team concluded that the TOE has met the assurance requirements of ASE_INT.1. Therefore, a **pass** verdict has been issued for this assurance component.

4.1.4 ASE_OBJ.1 – Security objectives

71 The evaluator reviewed the security objectives section of the [LMF2_ST] to satisfy the evaluator elements of this assurance component. The [LMF2_ST] security objective section breaks the objectives out into security objectives for the TOE and security objectives for the environment.

72 The evaluator reviewed the mappings supplied by the developer in the [LMF2_ST] to see that all security objectives for the TOE are traced back to the identified threats to be countered by the TOE. The evaluator developed a table that contained the threats and objectives for the TOE. This table was used to determine that all threats for the TOE are being mapped to the objectives of the TOE and that all the objectives of the TOE are being used and mapped to the threats of the TOE. The evaluator's table was a check on the developer's generated table to determine that it was accurate with respect to the objectives and threats being listed and articulated elsewhere in the [LMF2_ST].

73 The same approach described in the above paragraph was used to determine that the objectives for the environment are traced backed to threats and assumptions not completely countered by the TOE. This approach again was used to verify a mapping that the developer provided in the [LMF2_ST].

74 The evaluator read each security objective in the [LMF2_ST] to make a determination that each objective is clearly stated and understandable.

75 As part of determining the tracings discussed above the evaluator was also reviewing the rationale that was being given by the developer as to why a particular mapping was suitable to cover an identified threat and/or assumption. The rationale given by the developer explained how the objectives are suitable to cover the threats and/or assumptions stated in the [LMF2_ST].

76 ***ASE_OBJ.1 Verdict:***

77 The evaluation team concluded that the TOE has met the assurance requirements of ASE_OBJ.1. Therefore, a **pass** verdict has been issued for this assurance component.

4.1.5 ASE_PPC.1 – PP claims

78 The evaluator used the [LMF2_ST] and the [TFF_PP] to perform the activities required for the PP claims work units. It was determined by reviewing the [LMF2_ST] that compliance to the [TFF_PP] is being claimed. In addition, the [LMF2_ST] is claiming conformance to part 2 and part 3 of the CC.

79 The evaluator compared the assumptions, threats, objectives, functional requirements, and assurance requirements of both the [LMF2_ST] and the [TFF_PP]. This activity was performed to determine if the assumptions, threats, objectives, functional and assurance requirements were being re-stated correctly or if operations were being performed and identified correctly on these items.

80 The evaluator made sure that the objectives as stated in the [LMF2_ST] with any applicable operations performed are keeping the intent of the objectives as specified in the [TFF_PP]. The evaluator made sure that the functional requirements as stated in the [LMF2_ST] with any applicable operations performed on the functional requirement are keeping the intent of the functional requirements as stated in the [TFF_PP]. The evaluator determined that the functional requirement as specified in the [LMF2_ST] could meet the requirement as specified in the [TFF_PP] and would also meet the requirement intent as specified in the CC.

81 ***ASE_PPC.1 Verdict:***

82 The evaluation team concluded that the TOE has met the assurance requirements of ASE_PPC.1. Therefore, a **pass** verdict has been issued for this assurance component.

4.1.6 ASE_REQ.1 – IT security requirements

83 The evaluator examined both the [LMF2_ST] and the [TFF_PP] to accomplish the evaluator activities for ASE_REQ.

84 Part of the examination of the requirements of the [LMF2_ST] was to see if the functional requirements are transcribed from the [TFF_PP] correctly. The functional requirements in the [LMF2_ST] and the [TFF_PP] were compared during examination of the requirement sections. If the functional requirement was not exactly transcribed from the [TFF_PP] then the operations performed on the functional requirements in the [LMF2_ST] were examined. The examination of the operation was used to determine if the operation fit within the bounds for that specific functional requirement as stated in the CC and the [TFF_PP]. Also part of the comparison of the functional requirements involved making sure that those operations that are performed in the [LMF2_ST] are properly identified.

85 The same procedure as stated above was used for the assurance requirement section of the [LMF2_ST]. The only difference was that the [LMF2_ST] added two assurance maintenance components. The evaluator checked to make sure that these assurance maintenance components were identified as not being part of the EAL 2 package and that these assurance requirements did not exist in the [TFF_PP].

86 The dependency analysis and rationale were used from the [TFF_PP]. Since the LMF2_ST is only using the functional requirements from the [TFF_PP] and not any additional ones the same analysis and rationale is valid for the [LMF2_ST]. The evaluator did examine the impact of leaving out specific functional requirements because the TOE was not offering remote administration. The exclusion of these requirements did not violate any dependency relationships. The [LMF2_ST] is using the whole EAL 2 package so there are no dependency issues with the assurance level. The evaluator did examine the dependencies of the maintenance components being used and observed that not all

dependencies are being satisfied. The developer gave proper rationale for not satisfying all dependencies.

87 The examination of the functional requirement section of the [LMF2_ST] involved checking for a statement of Strength of Function (SOF) and checking that the appropriate requirements contained a SOF statement. The SOF rationale was examined to determine if it was appropriate for the TOE and the environment of the TOE.

88 The rationale for the assurance and functional requirements was examined. The examination of this rationale was undertaken to determine if the security requirements are able to meet the objectives specified in the [LMF2_ST]. The evaluator was also examining the IT security requirements rationale to see if there is a demonstration of how the security requirements are a mutually supportive and consistent whole. After reviewing the requirements rationale it could be seen that the requirements where mutually supportive in satisfying the security objectives of the [LMF2_ST]. The evaluator examined the security requirements, objectives, the mappings in the [LMF2_ST], and the requirement dependencies in achieving the satisfaction of mutually supportive and consistent whole. The requirements supported each other by setting up a security perimeter for the TOE that is non-bypassable and that maintains a separate domain that only the TOE executes in. This allows the security functions that enforce the traffic filter and auditing rules of the TOE to execute without interference. Further the non-bypassable separate domain of the TOE only allows for those authorized to administer the TOE to do so. Therefore, the requirements in the [LMF2_ST] are a mutually supportive and consistent whole because the requirements are structured and support each other, in a non-contradictory way, to enforce the security objectives expressed in the [LMF2_ST].

89 ***ASE_REQ.1 Verdict:***

90 The evaluation team concluded that the TOE has met the assurance requirements of ASE_REQ.1. Therefore, a **pass** verdict has been issued for this assurance component.

4.1.7 ASE_SRE.1 – Explicitly stated IT security requirements

91 There are no explicitly stated IT security requirements.

92 ***ASE_SRE.1 Verdict:***

93 The evaluation team concluded that the TOE has met the assurance requirements of ASE_SRE.1. Therefore, a **pass** verdict has been issued for this assurance component.

4.1.8 ASE_TSS.1 – TOE summary specification

94 The evaluator examined the TOE summary specification section of the [LMF2_ST]. The evaluator examined the summary specification for the functional and assurance requirements.

95 The evaluator examined each security function to determine that it was to a level of detail that summarized what the security functionality is and if the security function could satisfy the security functional requirement that it was mapped back to. The evaluator also

checked that each security functional requirement had at least one security function being mapped to it.

96 The mapping of assurance measures to assurance components were examined. The evaluator checked to make sure that each assurance component had a measure mapped to it and the measure is appropriate to satisfy a particular assurance component.

97 To accomplish the examination of the TOE summary specification the evaluator came up with their own tables to supplement and check the consistency of the tables supplied in the [LMF2_ST].

98 **ASE_TSS.1 Verdict:**

99 The evaluation team concluded that the TOE has met the assurance requirements of ASE_TSS.1. Therefore, a **pass** verdict has been issued for this assurance component.

4.2 Configuration Management Results

100 The objectives of this activity are to determine whether Lucent has clearly identified the TOE and its associated configuration items.

4.2.1 ACM_CAP.2 – CM capabilities

101 The evaluator checked and examined [LMF2_ACM] and [LMF2_ST]. The evaluator examined [LMF2_ST] to understand the definition of the TOE and then checked [LMF2_ACM] to determine if the Configuration Items (CI) identified made sense given the TOE definition. The evaluator checked that the TOE was uniquely referenced by version and build number and that the TOE software and hardware were labeled with its reference. The evaluator checked that the TOE references were consistent. The evaluator examined the CI and determined that the list identified items that compose the TOE and that the CI were uniquely identified. The [LMF2_ACM] provided a description of how each item was uniquely identified. As a result of these activities, the evaluator determined that all requirements for this activity were satisfied.

102 ***ACM_CAP.2 Verdict:***

103 The evaluation team concluded that the TOE has met the assurance requirements of ACM_CAP.2. Therefore, a **pass** verdict has been issued for this assurance component.

4.3 Delivery and Operation Results

104 The objectives of this activity are:

- to determine whether the delivery documentation describes all procedures used to maintain integrity when distributing the TOE to the user's site; and
- to determine whether the procedures and steps for the secure installation, generation, and start-up of the TOE have been documented and result in a secure configuration.

4.3.1 ADO_DEL.1 – Delivery Procedures

105 The evaluation team checked and examined the following evidence [LMF2_IGS] and [LMF2_ST]. The evaluator read through the [LMF2_IGS] and based on the procedures presented and the low risk environment for the TOE as specified in the [LMF2_ST], it was determined that shrink-wrapped CDs with unique software license keys was sufficient for secure delivery of the TOE. The evaluator did verify the procedures for delivery by calling the 1-800 Customer Care number and querying the help desk. By performing these activities, the evaluation team has determined that all requirements for this component have been satisfied.

106 ***ADO_DEL.1 Verdict:***

107 The evaluation team concluded that the TOE has met the assurance requirements of ADO_DEL.1. Therefore, a **pass** verdict has been issued for this assurance component.

4.3.2 ADO_IGS.1 – Installation, generation, and start-up procedures

108 The evaluation team checked and examined the following evidence [LMF2_IGS] and [LMF2_MAN6]. The evaluator did find that the procedures for secure installation, generation, and startup were provided. The [LMF2_IGS] section 3.0 identifies components, such as documentation, software, and hardware, provided by the vendor with the purchase of the LMF to verify that all components required for installation have been received. The evaluation team determined that the evidence does describe the necessary steps for secure installation, generation, and start-up of the TOE because the following were described: security safeguards for the SMS, steps to securely install the SMS, the brick and Windows NT, descriptions of configuration considerations to secure the TOE, and descriptions of required rule sets. In addition, the procedures presented in [LMF2_IGS] were verified through testing activities conducted under the ATE_IND work units. By performing these activities, the evaluation team has determined that all requirements for this component have been satisfied

109 ***ADO_IGS.1 Verdict***

110 The evaluation team concluded that the TOE has met the assurance requirements of ADO_IGS.1. Therefore, a **pass** verdict has been issued for this assurance component.

4.4 Development Results

111 The objectives of this activity are:

- to determine whether Lucent has provided an adequate description of the security functions of the TOE and whether the security functions provided by the TOE are sufficient to satisfy the functional requirements of the ST;

- to determine whether the high-level design is sufficient to satisfy the functional requirements of the ST, provides a description of the TSF in terms of major structural units with functional coherence, and is a realization of the functional specification; and

- to determine whether Lucent has correctly and completely implemented the requirements of the ST and functional specification in the high-level design.

4.4.1 ADV_FSP.1 – Informal functional specification

112 The initial approach to trying to satisfy this assurance component was for the evaluator to determine the boundaries of the TOE independently and then determine if the boundary described in the functional specification is accurate. In determining the boundary of the TOE the evaluator used the [LMF2_ST] and the supporting descriptions of the TOE provided in the high-level design, functional specification, and the user and administrator manuals that are part of the TOE. Through examination of these documents the evaluator determined that the external interfaces to the TOE are the external and internal networking interfaces and the GUIs supplied by the NT workstation.

113 The evaluator used the administrator guidance of the TOE along with the installation, generation, and start-up document to help in the assessment of this assurance component. The other documents that were used were the [LMF2_FSP], [LMF2_RCR], and the [LMF2_ST]. Through the evaluation of the evidence it was determined that the functional specification was composed of the [LMF2_FSP] and the TOE documentation that comes with the TOE.

114 The [LMF2_FSP] helps satisfy this assurance component by describing the security functions of the TOE and gives a description of the external interfaces of the TOE. The [LMF2_FSP] references several reference manuals that come with the TOE. These manuals help satisfy the functional specification assurance requirement by further defining and describing the external interfaces of the TOE. These reference manuals describe the GUI interface that the TOE provides and describe the interfaces to the management of the auditing, accounts, and firewall capability of the TOE. The developer is using RFCs for the description of the networking interfaces of the TOE. The RFCs describe the protocol interface that is used to control the networking interfaces.

115 The evaluation of the functional specification was tied very closely to the evaluation activities of the correspondence evidence. The reason for this is that the developer provided mappings that allowed the evaluator to map security functional requirements to security functions and security functions to TSF interfaces. These let the evaluator determine if the security functionality that was being mapped to security functional requirements was valid to satisfy the security functional requirement.

116 Using the correspondence mappings the evaluator examined the security functions that were being mapped onto security functional requirements. By doing this activity the evaluator was able to see if the security functionality actually existed in the TOE to support the security functional requirement. The evaluator was further able to use the correspondence mappings, supplied by the developer, to determine what external interfaces (i.e., TSF interfaces) could directly or indirectly affect the security functionality of the TOE. This allowed the evaluator to determine if there is some external interface that allows the evaluation team to test the security functionality of the TOE.

117 Through examination of the correspondence mappings and the description of the security functions it can be seen that the TOE has all the necessary security functionality to satisfy the security functional requirements in the [LMF2_ST].

118 ***ADV_FSP.1 Verdict:***

119 The evaluation team concluded that the TOE has met the assurance requirements of ADV_FSP.1. Therefore, a **pass** verdict has been issued for this assurance component.

4.4.2 ADV_HLD.1 – Descriptive high level design

120 The evaluator while examining the high-level design looked to see if it was in terms of major structural units. The evaluator also examined the high-level design to determine if it contained the major structural units to satisfy the security functional requirements in the [LMF2_ST]. The high-level design for this evaluation is in terms of subsystems.

121 The correspondence document, [LMF2_RCR], was an important document in the satisfaction of this assurance component. The correspondence mappings provide a mapping of the security functions onto subsystems. This allowed the evaluator to determine if the subsystem contained the proper functionality to satisfy the security function(s) being mapped to the subsystem. This also allowed the evaluator to determine if there were enough subsystems to cover all the security functionality (security functions and security functional requirements) being described in the [LMF2_ST].

122 The [LMF2_HLD], the high-level design document, was the primary document reviewed to satisfy this assurance component. The document has individual sections that describe each subsystem. The description given in each section describes the security functionality that the subsystem supports. The high-level design of the TOE described an architecture that allows for the satisfaction of the security functional requirements that are present in the [LMF2_ST]. Further the high-level design shows the information flow and relationships between the different subsystems of the TOE.

123 The evaluation team does not believe it is the intent of EAL 2 high-level design to describe all interfaces to the subsystems. The evaluation team believes that for EAL 2 it is more appropriate that the relationship of the subsystems should be shown in a high-level design. The identification of all interfaces to the subsystems is a different level of abstraction which is more appropriate in a low-level design document and not in a high-level design document. The evaluation team believes that the [LMF2_HLD] meets the intent of the ADV_HLD.1 component by showing the relationships and flow of information between the subsystems.

124 ***ADV_HLD.1 Verdict:***

125 The evaluation team concluded that the TOE has met the assurance requirements of ADV_HLD.1. Therefore, a **pass** verdict has been issued for this assurance component.

4.4.3 ADV_RCR.1 – Informal correspondence demonstration

126 The evaluator determined that for this EAL 2 evaluation that there are four different levels of abstraction for the TSF. These different abstractions are the security functional requirements, the security functions, the functional specification (the TSFIs), and the high-level design.

127 The main evidence examined for this assurance component was [LMF2_RCR], [LMF2_HLD], [LMF2_ST], TOE documents (administrator, installation, etc.) and [LMF2_FSP]. These documents contained all the relevant abstractions of the TSF.

128 The [LMF2_RCR] document supplied all the relevant mappings that are required for this assurance component. The correspondence document mapped security functions to security functional requirements. It mapped security functions to TSFIs. It further mapped security functions onto subsystems. With all these mappings the evaluator had enough information to determine which TSFI was being used to satisfy which security functional requirements and which subsystem is responsible for the security functionality. These mappings allow for a correspondence between the functional requirements, security functions, TSFI, and the high-level design.

129 **ADV_RCR.1 Verdict:**

130 The evaluation team concluded that the TOE has met the assurance requirements of ADV_RCR.1. Therefore, a **pass** verdict has been issued for this assurance component.

4.5 Guidance Documents Results

131 The objectives of this activity are:

- to determine whether the administrator guidance to system administrative personnel describes how they administer the TOE in a secure manner; and
- to determine whether the user guidance describes the security functions and interfaces provided by the TSF for non-administrative users and whether this guidance provides instructions and guidelines for the secure use of the TOE.

4.5.1 AGD_ADM.1 – Administrator guidance

132 The evaluation team examined the following evidence [LMF2_MAN6], [LMF2_MAN5], [LMF2_MAN2], [LMF2_MAN1], [LMF2_ADM], [LMF2_FSP], [LMF2_IGS] and [LMF2_ST]. The administrator guidance did contain a description of the security functionality that is visible at the administrator interface. The entire interface is a GUI interface in which the administrator is required to login and provide an account identification and password. The guidance identified and described the interfaces to configure the information flow policies, manage the audit trail to include selecting logged events, reviewing the log files, and configuring the “halt traffic if the audit log is full” feature, management of user accounts on Windows NT, and setting the system clock. The administrator guidance did describe how to operate the TOE in a secure environment as described in the [LMF2_ST] and provided warnings and tips about functions and parameter settings that should be controlled. The administrator guidance described security parameters under the control of the administrator indicating appropriate secure values. The administrator guidance adequately described the following security-relevant events relative to the administrative functions that need to be performed: audit trail overflow, system crashes and recovery, time changes, security policy flow changes, and user account changes. The administrator guidance was compared to the development evidence, installation, generation and startup procedures, and ST and was found to be consistent with these documents. Since the [LMF2_ST] does not include requirements on the IT environment, the evaluator determined that descriptions concerning the IT

security requirements was not applicable. As a result of these activities, the evaluator determined that all requirements for this activity were satisfied.

133 ***AGD_ADM.1 Verdict:***

134 The evaluation team concluded that the TOE has met the assurance requirements of AGD_ADM.1. Therefore, a **pass** verdict has been issued for this assurance component.

4.5.2 AGD_USR.1 – User guidance

135 The LMF does not allow users to interact directly with the security functionality of the TOE. Therefore, there is no requirement to provide any user documentation. The evaluation team determined that this assurance component as not applicable.

136 ***AGD_USR.1 Verdict:***

137 The evaluation team concluded that the assurance requirements of AGD_USR.1 was not applicable and that the assurance component satisfied. Therefore, a **pass** verdict has been issued for this assurance component.

4.6 Testing Results

138 The objectives of this activity are:

- to determine whether the test coverage evidence shows correspondence between the tests identified in the test documentation and the functional specification;
- to determine whether Lucent's functional testing demonstrates that all security functions perform as specified; and
- to determine whether the TOE behaves as specified and to gain confidence in Lucent's test results by independently testing a subset of the TSF and by performing a sample of the developer's tests.

4.6.1 ATE_COV.1 – Evidence of coverage

139 The evaluation team examined the following evidence [LMF2_COV] [LMF2_PRO], [LMF2_FAIL], [LMF2_REG], [LMF2_VIR], [LMF2_URL], and [LMF2_UMA]. The coverage analysis presented a table that accurately mapped tests to security functions and SFRs. The mapping revealed that not all security functions were tested which is acceptable for this assurance component.

140 ***ATE_COV.1 Verdict:***

141 The evaluation team concluded that the TOE has met the assurance requirements of ATE_COV.1. Therefore, a **pass** verdict has been issued for this assurance component.

4.6.2 ATE_FUN.1 – Functional testing

142 The evaluation team checked and examined the following test evidence provided by the vendor: [LMF2_COV], [LMF2_PRO], [LMF2_FAIL], [LMF2_REG], [LMF2_VIR],

[LMF2_URL], [LMF2_UMA] and the [LMF2_ST]. The test evidence included test plans, test procedures, expected test results, and actual test results. The test evidence was not specifically designed for the Common Criteria evaluation. The test documentation supplied by Lucent does not explicitly identify security functions as stated in the Security Target but rather describes the areas of LMF functionality that is being tested. As a result, the evaluation team examined the test plans and the test coverage analysis to determine which security functions were being tested. The test configurations described in the test evidence did not exactly match the configuration identified in the [LMF2_ST] and [LMF2_IGS]. However, the network architecture described was consistent with that described in the [LMF2_IGS]. For each test case a purpose was provided that described the purpose of the test case. The descriptions are adequate to inform the tester and evaluator of the security functionality that the test will be exercising. Because the test procedures identified the initial conditions, steps for conducting the tests, and expected behavior, the evaluator determined that sufficient instructions were provided to establish reproducible results. The expected test results in the test documentation were consistent with the actual test results provided.

143 ***ATE_FUN.1 Verdict:***

144 The evaluation team concluded that the TOE has met the assurance requirements of ATE_FUN.1. Therefore, a **pass** verdict has been issued for this assurance component.

4.6.3 ATE_IND.2 – Independent testing – sample

145 The evaluation team documented the evaluator's test plan, procedures, expected results, and actual results in [LMF2_IND]. Before independent testing proceeded the evaluation team installed and configured the LMF using [LMF2_IGS]. The evaluation team tested the default configuration to ensure that all information flows were denied. The evaluation team produced a sample test subset by recreating tests found in [LMF2_REG]. The evaluators chose tests that tested audit overflow and information flow through the brick. The evaluators conducted additional independent tests that tested the Windows NT interfaces for account management and audit management. In addition, a different audit overflow test was created. Additionally, information flow rules were tested as part of penetration testing.

146 ***Independent Testing Details***

147 The approach to the independent testing effort was to ensure that Security Functional Requirements (SFRs) as stated in the [LMF2_ST] operated as specified. Specific emphasis was placed on those functions that enforced the information flow control security policy, FDP_IFF.1 and FDP_IFC.1. Further the evaluation team used the documents that were part of the [LMF2_FSP] to conduct some of its independent tests. The [LMF2_FSP] gave indications of potential interfaces to test, the administrator and networking interfaces. Additionally, the evaluators wanted assurance that all required audit events were successfully captured and recorded by the TOE.

148 Another area of concern was the FAU_STG.1 and FAU_STG.4, two new requirements implemented by the TOE to ensure that all traffic is denied when an audit record cannot be generated (i.e. when the audit logs are full).

149 It is important to note that the evaluation team was able to determine that the developer performed a significant level of testing of the security functions of the LMF. However, none of this testing was performed with the product installed and configured in the evaluated configuration, as stated in the [LMF2_IGS]. Therefore, to provide assurance that the product will perform as specified in the [LMF2_IGS] document, the evaluation team performed an extended set of independent functional testing.

150 The following actions were taken to prepare the laboratory for testing:

- [LMF2_SOFT] was installed upon the host machine in accordance with [LMF2_IGS].
- A series of administrator and user accounts were created on the TOE, and on the internal and external network PCs.

151 ***Testing Conclusions***

152 The complete set of functional tests performed as expected. All independent testing formulated and performed by the evaluator produced actual results that mirrored expected results. Therefore, the independent functional testing of the TOE produced positive results and all functions tested performed as expected and the tested SFRs have been correctly and completely implemented.

153 ***ATE_IND.2 Verdict:***

154 The evaluation team concluded that the TOE has met the assurance requirements of ATE_IND.2. Therefore, a **pass** verdict has been issued for this assurance component.

4.7 Vulnerability Assessment Results

155 The purpose of the vulnerability assessment activity is to determine the exploitability of flaws or weaknesses in the TOE in the intended environment. This determination is based upon analysis performed by Lucent, and is supported by evaluator penetration testing.

4.7.1 AVA_SOF.1 – Strength of TOE security functions

156 The evaluation team examined the following evidence [LMF2_ST], [LMF2_ADM], [LMF2_HLD], [LMF2_FSP], [TFF_PP] and [LMF2_IGS]. The [TFF_PP] states that the minimum SOF level of SOF-basic shall apply to the FIA_UAU.1, FIA_UAU.4 and FCS_COP.1 SFRs. Because the TOE in the evaluated configuration does not provide remote administration capabilities or interact with authorized external IT entities, the only applicable SFR was determined to be FIA_UAU.1. The [LMF2_ST] only identifies one SFR, FIA_UAU.1, as having a SOF claim expressed as a metric. [LMF2_ADM] provides the SOF analysis that the probability of guessing a password with the correct security policy set for the administrator account is 8.7919 x 10-9. This figure satisfies the metric for the probability that authentication data can be guessed is no greater than one in a million, which is the stated requirement in the [TFF_PP] and [LMF2_ST]. The evaluator analyzed the [LMF2_ST], [LMF2_HLD], and [LMF2_FSP] documents to search for security mechanisms that are either probabilistic or permutational. It was determined that the identification and authentication mechanism used by the

administrator to authenticated to the SMS is the only security mechanism within testing scope that has these properties.

157 ***AVA_SOF.1 Verdict:***

158 The evaluation team concluded that the TOE has met the assurance requirements of AVA_SOF.1. Therefore, a **pass** verdict has been issued for this assurance component.

4.7.2 AVA_VLA.1 – Vulnerability analysis

159 The evaluation team examined the following evidence [LMF2_AVA], [TFF_PP], [LMF2_IGS], [LMF2_ST], and the test results in [LMF2_IND] of the evaluator tests conducted as part of completing ATE_IND independent testing. The evaluators determined that vulnerability analysis performed by the vendor did consider relevant information (e.g., CERT advisories, appendix A of the [TFF_PP]) to search for obvious vulnerabilities. The vendor's analysis identified vulnerabilities and provided rationale for each vulnerability that described why the vulnerability was not exploitable in the intended environment for the TOE. The arguments provided are consistent with TOE description in the ST and guidance for administering the system.

160 ***Penetration Testing Details***

161 The evaluation team produced [LMF2_PEN] which describes the penetration tests conducted by the evaluation team. The test configuration used was the exact same configuration used for independent testing (ATE_IND.2). The penetration testing of the LMF was broken down into the following areas:

- Testing for the existence of vulnerabilities identified in Appendix A of the [TFF_PP].
- Testing for the existence of vulnerabilities identified in the vendor's vulnerability analysis, the [LMF2_AVA] document.
- Testing and independent analysis for bypassability through functionality contained within the Network Interface Card's that form part of the TOE.
- Testing for additional vulnerabilities that may be relevant to the TOE. These vulnerabilities were identified by searching vulnerability advisories and databases at various web sites.

162 The evaluation team used protocol analyzers and CSC's proprietary Hydra Security Toolset to perform the penetration tests. These tests covered the following: IP spoofing, UDP attacks, ICMP vulnerability, IP Loose Source Routing Option vulnerability, fragmentation attacks, and OS race conditions. The evaluation team successfully completed the vulnerability tests and found the TOE to operate as expected. The TOE was not exploitable in the evaluated configuration.

163 ***AVA_VLA.1 Verdict:***

164 The evaluation team concluded that the TOE has met the assurance requirements of AVA_VLA.1. Therefore, a **pass** verdict has been issued for this assurance component.

4.8 Assurance Maintenance Results

165 The purpose of this activity is to determine if Lucent has defined a set of procedures that can be applied to provide confidence that the assurance established in the TOE can be maintained.

4.8.1 AMA_AMP.1 – Assurance maintenance plan

166 The evaluator reviewed the [LMF2_AMP] and [LMF2_CAT] documents as part of this evaluation activity. The review of the [LMF2_AMP] document showed that Lucent has named an individual as the Developer Security Analyst (DSA) that has the authority and knowledge to conduct security impact analysis and to maintain the rating of the evaluated TOE.

167 The [LMF2_AMP] details what scope of changes are acceptable for rating maintenance, the life cycle of the TOE, the assurance maintenance cycle, the flaw remediation process, and the assurance maintenance procedures.

168 The [LMF2_AMP] describes what Lucent will do to maintain all the evaluation evidence so that the rating of the current evaluated TOE will be maintained and to help the next full evaluation of the TOE.

169 ***AMA_AMP.1 Verdict:***

170 The evaluation team concluded that the TOE has met the assurance requirements of AMA_AMP.1. Therefore, a **pass** verdict has been issued for this assurance component.

4.8.2 AMA_CAT.1 – TOE component categorisation report

171 The evaluator reviewed the [LMF2_CAT], [LMF2_HLD], and the [LMF2_FSP] as part of this evaluation activity. The evaluator used the [LMF2_HLD] and the [LMF2_FSP] to determine if the [LMF2_CAT] was categorizing all the TSFIs and subsystems described in the [LMF2_FSP] and [LMF2_HLD].

172 After review of the [LMF2_CAT] it was determined that the developer had categorized all the TSFIs and subsystems in a manner that would allow the DSA to perform security impact analysis on the TOE. This was accomplished in the [LMF2_CAT] by labeling TSFIs and subsystems as TSF-enforcing and further indicating if those labeled as TSF-enforcing were security critical or security supporting. Further the [LMF2_CAT] document described the categorization method and re-categorization method being used for the TOE. The [LMF2_CAT] listed the development tools for the TOE. This will allow the DSA to determine if a modification to a development tool will affect the assurance of the TOE.

173 ***AMA_CAT.1 Verdict:***

174 The evaluation team concluded that the TOE has met the assurance requirements of AMA_CAT.1. Therefore, a **pass** verdict has been issued for this assurance component.

5 CONCLUSIONS AND RECOMMENDATIONS

175 The TOE was evaluated against the [LMF2_ST]. The assurance component verdicts presented in Chapter 4 of this report received final evaluation verdicts of **Pass**. Therefore, the evaluation team assigns an overall Pass verdict for satisfying the evaluator action elements defined for EAL 2. The ST was found to be conformant to [TFF_PP]. As defined by [CC_PART1] Chapter 5, the TOE was found to be Part 2 conformant, Part 3 conformant, and conformant to PP. The evaluation team recommends that an EAL 2 certificate rating be issued for the TOE.

6 LIST OF ACRONYMNS AND GLOSSARY OF TERMS

176 The following acronyms are used throughout this document.

ARP	Address Resolution Protocol
CC	Common Criteria
CCEL	Common Criteria Evaluation Laboratory
CCEVS	Common Criteria Evaluation and Validation Scheme
CEM	Common Evaluation Methodology
CI	Configuration Items
CSC	Computer Sciences Corporation
DSA	Developer Security Analyst
EAL	Evaluation Assurance Level
EDR	Evaluation Discovery Report
ETR	Evaluation Technical Report
FA	Firewall Appliance
GUI	Graphical User Interface
IP	Internet Protocol
LAN	Local Area Network
LMF	Lucent Managed Firewall
MRA	Mutual Recognition Arrangement
NES	Netscape Enterprise Server
NIAP	National Information Assurance Program
NIST	National Institute of Science & Technology
NSA	National Security Agency
OR	Observation Report
OS	Operating System
PP	Protection Profile
RAD	Remote Administration Daemon
RAP	Remote Administration Application
SAR	Security Assurance Requirement
SFR	Security Functional Requirements

SMS	Security Management Server
SOF	Strength of Function
ST	Security Target
TCP	Transport Control Protocol
TCSEC	Trusted Computer Systems Evaluation Criteria
TEF	TTAP Evaluation Facility
TOE	Target of Evaluation
TSC	TOE Scope of Control
TSF	TOE Security Functions
TSFI	TSF Interface
TTAP	Trust Technology Assessment Program
VPN	Virtual Private Network

7 PROBLEM REPORTS

7.1 Evaluation Discovery Reports

This section of contains all EDRs raised as a result of work performed during the evaluation. Table 5 provides the EDRs unique identifier, the work package in which the problem was discovered, a brief summary of the problem, and their status.

Table 5: List of Evaluation Discovery Reports

Identifier	Work Package	Title	Status
LMF2_EDR_001	ST Evaluation	Observations on Security Target	Closed
LMF2_EDR_002	Configuration Management	Observations on the Configuration Management Documentation	Closed
LMF2_EDR_003	Testing	Test coverage analysis needs updating to reflect LMF 4.0 testing	Closed
LMF2_EDR_004	Vulnerability Analysis	All sources used to search for “obvious” vulnerabilities must be identified	Closed
LMF2_EDR_005	Vulnerability Analysis	Password policy not described in guidance documentation.	Closed
LMF2_EDR_006	Vulnerability Analysis	The intended TOE operating environment is not defined.	Closed
LMF2_EDR_007	Vulnerability Analysis	Analysis provided for the IP loose source route option vulnerability indicates that the vulnerability may be exploitable in the TOE’s intended operating environment.	Closed
LMF2_EDR_008	Vulnerability Analysis	The analysis for the ARP Vulnerability foes not state how the vulnerability is not exploitable in the TOE’s intended environment.	Closed
LMF2_EDR_009	Vulnerability Analysis	The analysis for the Smurf Attack does not indicate that it is not exploitable in the TOE’s intended operating environment.	Closed
LMF2_EDR_010	Vulnerability Analysis	Inconsistencies exist within the [LMF2_AVA] document.	Closed
LMF2_EDR_011	Test	Deficiencies in [LMF2_IGS_1.0]	Closed
LMF2_EDR_012	Test	Deficiencies in [LMF2_ST dated 10/1/99]	Closed
LMF2_EDR_013	Development	Functional Specification	Closed
LMF2_EDR_014	Development	High-level Design	Closed
LMF2_EDR_015	Development	Representation correspondence	Closed
LMF2_EDR_016	Security Target	ST updates second round	Closed
LMF2_EDR_017	Guidance	Observations on Guidance Documentation	Closed
LMF2_EDR_018	Security Target	ST updates third round	Closed
LMF2_EDR_019	Development	FSP, HLD, and RCR	Closed
LMF2_EDR_020	Security Target	ALC_FLR & Version Numbers	Closed
LMF2_EDR_021	Test	Deficiency in [LMF2_IGS_1.0], Audit Policy needs updating.	Closed
LMF2_EDR_022	Maintenance	AMA_AMP.1 & AMA_CAT.1	Closed
LMF2_EDR_023	Flow Rules	Observation for the ETR	Closed

Identifier	Work Package	Title	Status
LMF2_EDR_024	Security Target	ST Development Version Numbers	Closed
LMF2_EDR_025	Maintenance	Touch ups	Closed

7.2 Observation Reports

This section of contains all ORs raised as a result of work performed during the evaluation. Table 6 provides the ORs unique identifier with corresponding Scheme identifier in parenthesis, as appropriate, a brief summary of the problem, and an indication of the problem's current status. The ORs that remain open do not impact the final verdict or results of this evaluation.

Table 6: Listing of Observation Reports

Identifier	Title	Status
LMF2_OR_001	Mandatory inclusion of an AUTHENTICATED SFP	Closed
LMF2_OR_002 (OR 149)	Clarification of what PP Compliance Means	Open
LMF2_OR_003 (OR 150)	High level design and all interfaces	Open
LMF2_OR_004	ADV_FSP.1 (TSF & TSFI)	Open
LMF2_OR_005	Certificate Maintenance	Open
LMF2_OR_006	TOE component categorisation report (AMA_CAT.1)	Open